Introduction to Safety Systems in Research Accelerators

SIL Selection

USPAS

June, 2004

Outline

- Review of SIL Allocation
- SIL Selection Tools

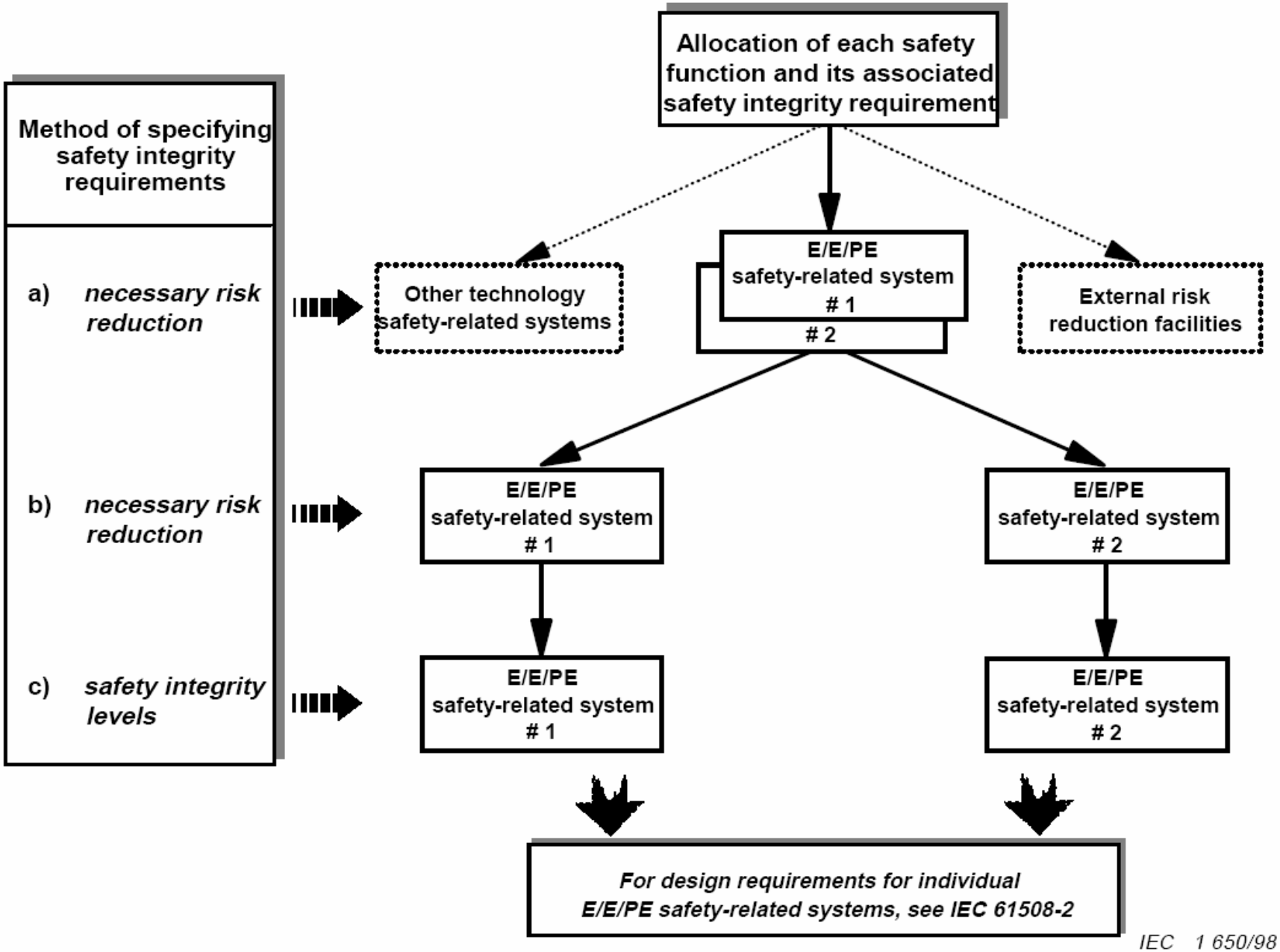
Review of SIL Allocation

- Allocation of safety functions to specific protection layers for the purpose of prevention, control or mitigation of hazards from the accelerator and its associated equipment;

- The allocation of risk reduction targets to safety instrumented functions.

Guide Lines for Determining Necessary Risk Reduction

- Guidelines from the appropriate safety regulatory authority;
- Discussions and agreements with the different parties involved in the application;
- Industry standards and guidelines;
- International discussions and agreements; the role of national and international standards are becoming increasingly important in arriving at tolerable risk criteria for specific applications;
- The best independent industrial, expert and scientific advice from advisory bodies;
- Legal requirements, both general and those directly relevant to the specific application.

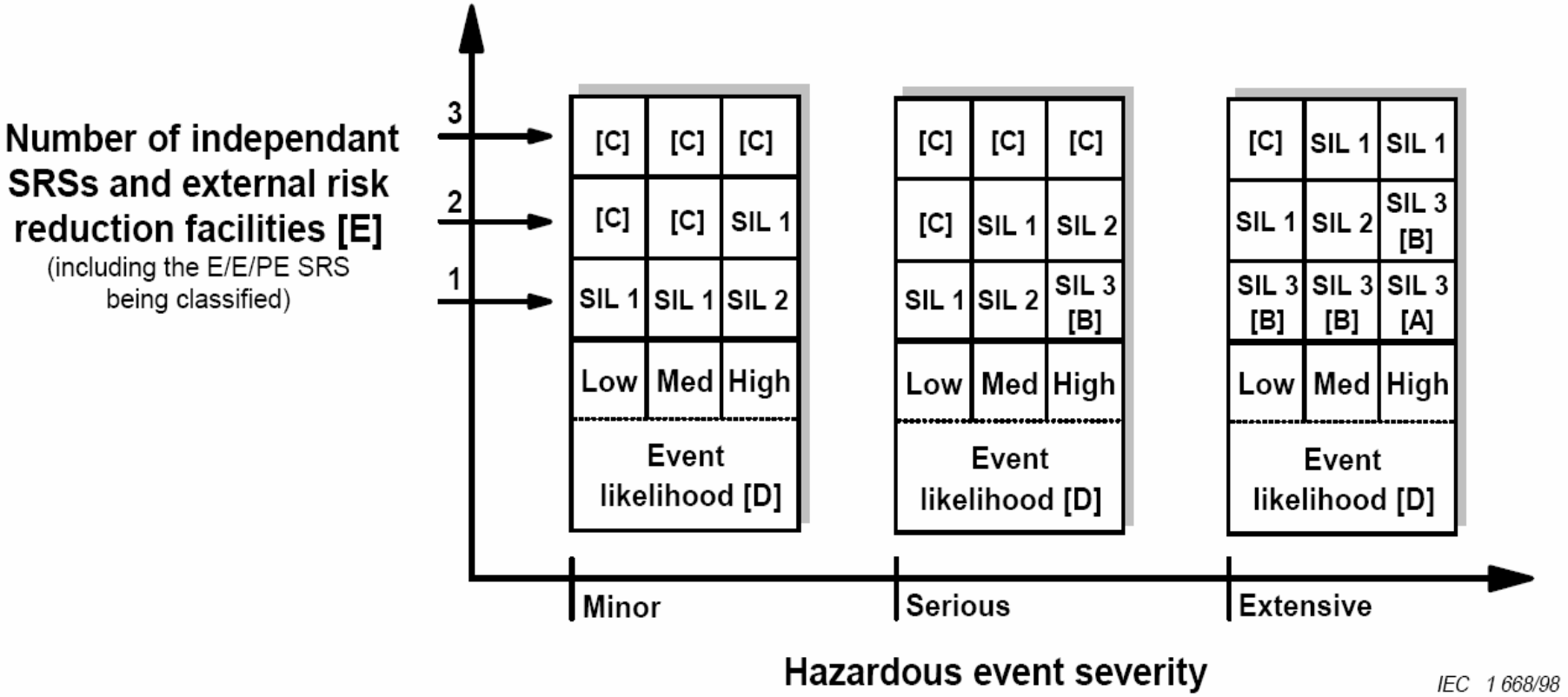

Method of specifying safety integrity requirements
a) necessary risk reduction
b) necessary risk reduction
c) safety integrity levels
Allocation of each safety function and its associated safety integrity requirement
Other technology safety-related systems
E/E/PE safety-related system # 1
2
External risk reduction facilities
E/E/PE safety-related system # 1
E/E/PE safety-related system # 2
E/E/PE safety-related system # 1
E/E/PE safety-related system # 2
For design requirements for individual E/E/PE safety-related systems, see IEC 61508-2
IEC 1 650/98

SIL Ranges

DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	**Average Probability of Failure on Demand**	**Risk Reduction**
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤ 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤ 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	**Frequency of Dangerous Failures Per Hour**
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Risk Matrix Approach



Risk Matrix

- **Risk matrix set up for hazard type**

External Risk Reduction	0						
Other Technology Based Systems	0						
SIL	0					User Defined	Range
Risk Matrix		Color code	Intolerable		0	4	
			Undesirable		4	5	
			Tolerable		5	7	
			Acceptable		7	>	
User Defined Likelihood							
Immanent	0	Frequent	3	2	1	0	
1day-1year	1	Probable	4	3	2	1	
1-10 years	2	Occasional	5	4	3	2	
Over life of facility	3	Remote	6	5	4	3	
100-1000 years	4	Unlikely	7	6	5	4	
>1000 years	5	Impossible	8	7	6	5	
			3	2	1	0	
		Consequences	Minimal	Marginal	Critical	Catastrophic	
			First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

Risk Matrix

- **External Risk Reduction and Other Methods Evaluated**

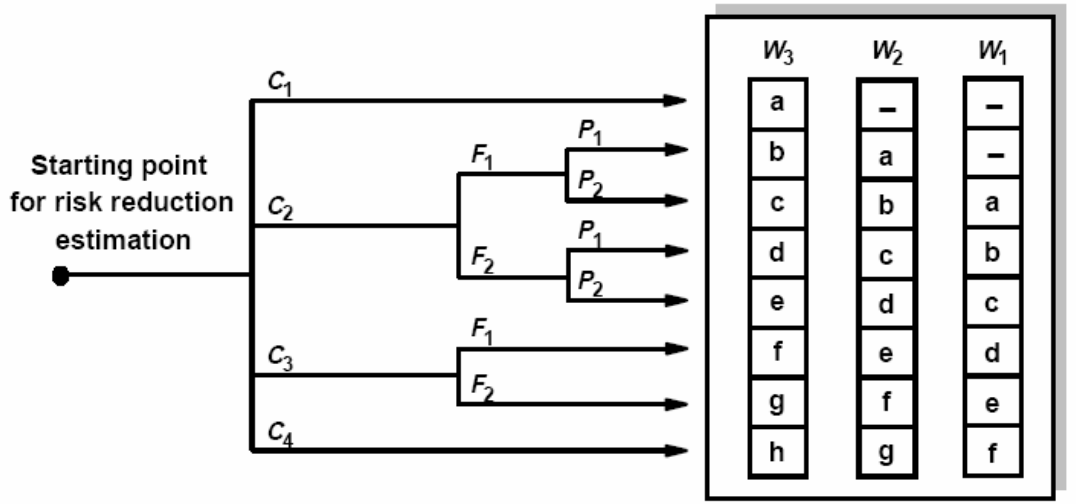
External Risk Reduction	2					
Other Technology Based Systems	1					
SIL	0					User Defined Range
Risk Matrix		Color code	Intolerable		0	4
			Undesirable		4	5
			Tolerable		5	7
			Acceptable		7	>
User Defined Likelihood						
Immanent	0	Frequent	6	5	4	3
1day-1year	1	Probable	7	6	5	4
1-10 years	2	Occasional	8	7	6	5
Over life of facility	3	Remote	9	8	7	6
100-1000 years	4	Unlikely	10	9	8	7
>1000 years	5	Impossible	11	10	9	8
			3	2	1	0
		Consequences	Minimal	Marginal	Critical	Catastrophic
			First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability

Risk Matrix

- Effect of SIL Levels Evaluated

External Risk Reduction	2						
Other Technology Based Systems	1						
SIL	3						User Defined Range
Risk Matrix		Color code	Intolerable		0	4	
			Undesirable		4	5	
			Tolerable		5	7	
			Acceptable		7	>	
User Defined Likelihood							
Immanent	0	Frequent	9	8	7	6	
1day-1year	1	Probable	10	9	8	7	
1-10 years	2	Occasional	11	10	9	8	
Over life of facility	3	Remote	12	11	10	9	
100-1000 years	4	Unlikely	13	12	11	10	
>1000 years	5	Impossible	14	13	12	11	
			3	2	1	0	
		Consequences	Minimal	Marginal	Critical	Catastrophic	
			First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

Risk Graph



a, b, c, d, e, f, g, h represent the necessary minimum risk reduction. The link between the necessary minimum risk reduction and the safety integrity level is shown in the table.

C = Consequence risk parameter

F = Frequency and exposure time risk parameter

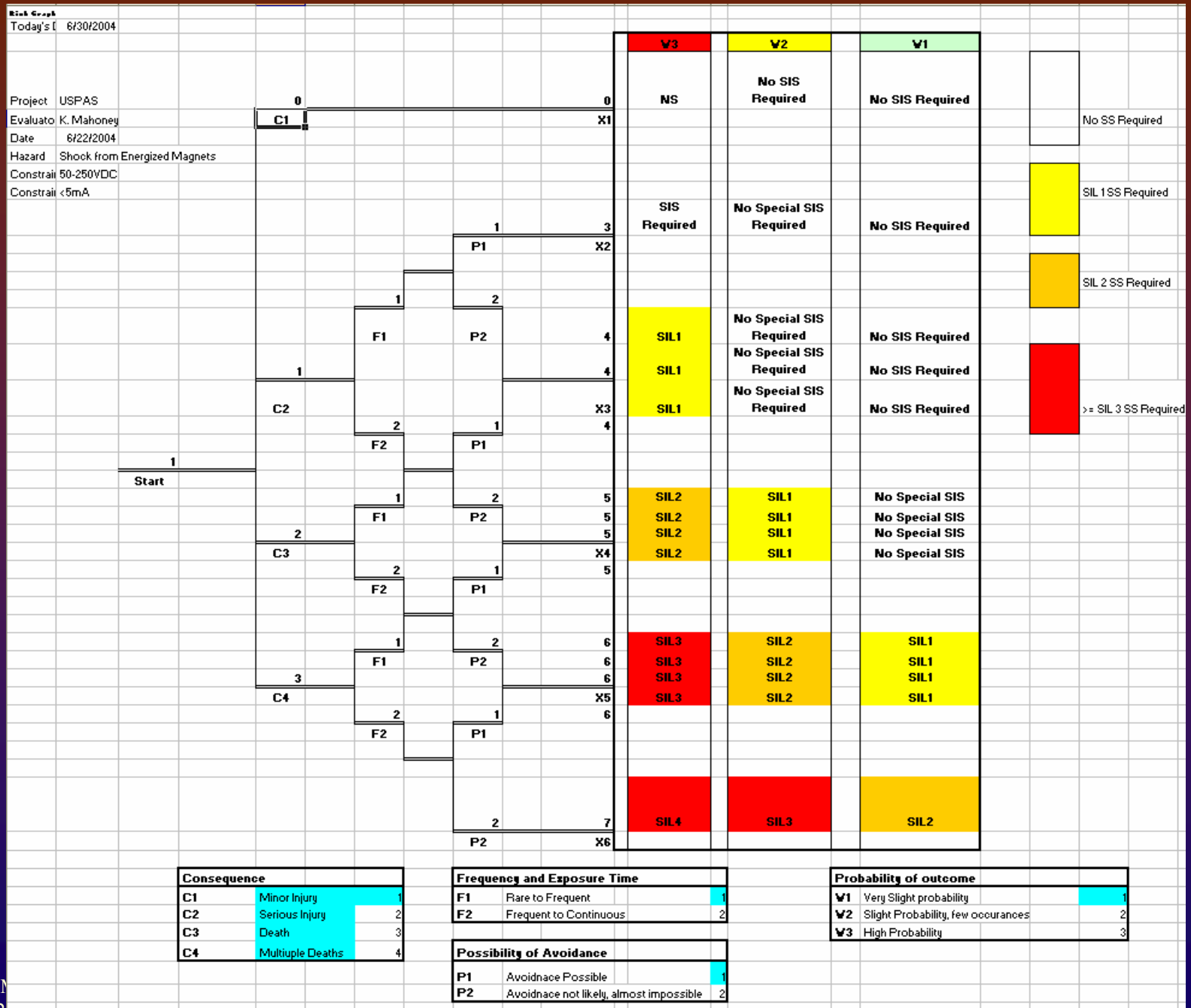
P = Possibility of avoiding hazard risk parameter

W = Probability of the unwanted occurrence

a, **b**, **c** ... **h** = Estimates of the required risk reduction for the SRSs

Necessary minimum risk reduction	Safety integrity level
–	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS is not sufficient

IEC 1 667/98


Risk Graph
Today's D 6/30/2004
Project USPAS
Evaluato K. Mahoney
Date 6/22/2004
Hazard Shock from Energized Magnets
Constrai 50-250VDC
Constrai <5mA
Start
C1
C2
C3
C4
F1
F2
P1
P2
X1
X2
X3
X4
X5
X6
W3
W2
W1
NS
No SIS Required
No SIS Required
SIS Required
No Special SIS Required
No SIS Required
SIL1
SIL2
SIL3
SIL4
No Special SIS
SIL 2
SIL1
No SS Required
SIL 1 SS Required
SIL 2 SS Required
>= SIL 3 SS Required
Consequence
C1 Minor Injury 1
C2 Serious Injury 2
C3 Death 3
C4 Multiuple Deaths 4
Frequency and Exposure Time
F1 Rare to Frequent 1
F2 Frequent to Continuous 2
Possibility of Avoidance
P1 Avoidnace Possible 1
P2 Avoidnace not likely, almost impossible 2
Probability of outcome
W1 Very Slight probability 1
W2 Slight Probability, few occurances 2
W3 High Probability 3

Quantitative

- Calculate Initial Risk using risk analysis tools
- Calculate the residual risk using
  - Event Tree
  - LOPA
- Calculate the necessary risk reduction to reach acceptable level
  - Requires numerical expression of acceptable risk

Quantitative Risk Reduction

$$RR = \frac{InherentRisk}{AcceptableRisk}$$

$$Safety\ Function\ PFDavg = \frac{1}{RR}$$